



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
|-----------------|-------------|----------------------|---------------------|------------------|

10/685,153

10/14/2003

Man-Pyo Hong

587-32

4789

7590 02/27/2007  
ROCCO S. BARRESE, ESQ.  
DILWORTH & BARRESE, LLP  
333 Earle Ovington Blvd.  
Uniondale, NY 11553

EXAMINER

NALVEN, ANDREW L

ART UNIT

PAPER NUMBER

2134

| SHORTENED STATUTORY PERIOD OF RESPONSE | MAIL DATE | DELIVERY MODE |
|--|-----------|---------------|
|--|-----------|---------------|

3 MONTHS

02/27/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

# Office Action Summary

Application No.

10/685,153

Applicant(s)

HONG ET AL.

Examiner

Andrew L. Nalven

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☐ Responsive to communication(s) filed on 14 October 2003.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-3 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1 and 2 is/are rejected.
- 7) ☒ Claim(s) 3 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.


## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 14 October 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

  
KAMBIZ ZAND  
PRIMARY EXAMINER

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 10/14/2003.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_.

### DETAILED ACTION

1. Claims 1-3 are pending.

#### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-3 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The cited claims provide a step of classifying a malicious script encryption method into three cases. Subsequently, the claim is directed to the obtaining of a decrypted script if the classifying step determines that the malicious script encryption method meets the first case, whereby the malicious script encryption method is an independent function. However, the claims fail to provide any steps to be taken if the classification step determines that the malicious script encryption method falls into the second or third class. Thus the claims are indefinite regarding these classes of malicious scripts.
3. In addition, with regards to claim 1, the phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Art Unit: 2134

4. Finally, with regards to claim 1, the limitation "the external codes" as found on lines 4-5 lacks antecedent basis.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenburg US Patent No. 5,696,822 in view of Nachenburg US Patent No. 6,851,057.

6. With regards to claim 1, Nachenburg '822 teaches classifying a malicious script encryption method into a case where a decryption function exists in malicious scripts and is an independent function that is not dependent on the external codes such as run time library (Nachenburg '822, column 8 lines 25-35, interrupts/instruction jumps determined), a case where a decryption function exists and is a dependent function that is dependent on external codes (Nachenburg '822, column 8 lines 25-35), and a case where a decryption function does not exist (Nachenburg '822, column 8 lines 25-51). Nachenburg '822 fails to teach extracting a call expression and a function definition for the function, executing or emulating the extracted call expression and function definition for the function and obtaining a decrypted script by putting a result value based on the execution or emulation into an original script at which an original call expression is

Art Unit: 2134

located. However, Nachenburg '057 teaches extracting a call expression and a function definition for the function, executing or emulating the extracted call expression and function definition for the function (Nachenburg '057, column 8 lines 5-33 and lines 55-67) and obtaining a decrypted script by putting a result value based on the execution or emulation into an original script at which an original call expression is located (Nachenburg '057, column 9 lines 47-65). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Nachenburg '057's method of extracting a call expression and function definition to emulate because it offers the advantage of allowing quick scanning by focusing scanning upon a main entry point of a file where a viral body is likely to reside (Nachenburg '057, column 2 lines 11-28).

7. With regards to claim 2, Nachenburg '822 as modified teaches that whether there exists the dependency of the decryption function on external codes is determined based on whether there exists the dependency for all codes within the decryption function on the external codes, whether actual parameters for decryption function call in all programs are constants, and whether only functions with no side effects in the decryption function are called (Nachenburg '822, column 8 lines 25-35. column 7 lines 53-67).

***Allowable Subject Matter***

Claim 3 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

The cited prior art, Nachenburg '057 and '822 teach methods of virus detection. However, the cited prior art fails to teach the determining that there is no dependency on external codes by determining if function  $F_i$  satisfies the formula:  $V_i \cap E_i = \Phi$  where  $V_i$  is a set of global variables defined or used in function  $F_i$  and is obtained using the formula  $V_i = A_i - D_i$  as set forth in claim 3. As a result, the cited prior art fails to anticipate or render obvious the above cited claim.

***Conclusion***

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.
9. Nachenburg US Patent No. 5,964,889 discloses a method to analyze a program for the presence of a computer virus by examining the opcode for faults.
10. Muttik et al US Patent No. 6,907,396 discloses a method of detecting a computer virus by patching instructions into an emulator.

Art Unit: 2134

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Andrew Nalven

ALN

  
KAMBIZ ZAND  
PRIMARY EXAMINER